AMENDMENTS TO THE SPECIFICATION AND ABSTRACT

Please replace the paragraph beginning at line 1 on page 1 with the following rewritten paragraph:

~~TITLE OF THE INVENTION~~

Group Formation/Management System, Group Management Device, and Member Device

Please replace the paragraph beginning at line 24 on page 4 with the following rewritten paragraph:

Also, a group management device of the present invention manages a group, and includes: a reception unit operable to receive, from a member device, a request for registration to the group; a judging unit operable, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, and to register the member device when judged in the affirmative; and a communication unit operable, when the judging unit judges in the affirmative, to output to the member device, common secret information unique to the group.

Please replace the paragraph beginning at line 24 on page 5 with the following rewritten paragraph:

Here, the group management device may further include a content storage unit operable to store therein a content key and an encrypted content which is encrypted by using the content key; and an encryption unit operable to encrypt the content key by using a key generated based on the common secret information, to generate an encrypted content key. The, ~~and the~~ communication unit may output the encrypted content and the encrypted content key to the member device.

Please replace the paragraph beginning at line 8 on page 6 with the following rewritten paragraph:

Also, in the member device, the requesting unit may request the group management device for delivery of the content, and the receiving unit may receive, from the group management device, an encrypted content generated by encrypting the content

using a content key, and an encrypted content key generated by encrypting the content key using ~~an encryption key~~ generated based on the common secret information. ~~The, and the~~ member device may further include a decryption unit operable to generate a decryption key corresponding to the same as the encryption key, based on the common secret information, to decrypt the encrypted content key using the decryption key to obtain a content key, and to decrypt the encrypted content using the content key to obtain a content.

Please replace the paragraph beginning at line 4 on page 7 with the following rewritten paragraph:

Also, a registration device of the present invention registers a member device in a group managed by a group management device, and includes: a holding unit operable to receive, from the group management device, and hold, common secret information unique to the group; and a notifying unit operable, when the registration device is connected to the member device, to notify the common secret information to the member device.

Please replace the paragraph beginning at line 24 on page 13 with the following rewritten paragraph:

Content storage unit 109 stores encrypted contents that are encrypted by using content keys. Moreover, although the method of acquiring contents is not the subject of the present invention and a description is thus omitted here, acquisition methods include, for example, acquiring contents using the Internet, broadcasts or the like, or acquiring contents from a recording medium such as a DVD.

Please replace the paragraph beginning at line 3 on page 22 with the following rewritten paragraph:

Moreover, although the above description relates here to CSI having been generated, when CSI has not ~~being~~ been generated, CSI is generated and transmitted to IC card 400 in the same manner as when playback apparatus 200 is registered.

Please replace the paragraph beginning at line 11 on page 25 with the following ~~rewritten paragraph:~~

Playback apparatus 200 is a computer system ~~the same~~similar to AD server 100, and a computer program is stored in the RAM or the hard disk unit of playback apparatus 200. Playback apparatus 200 carries out functions as a result of the microprocessor operating in accordance with the computer program.

Please replace the paragraph beginning at line 8 on page 27 with the following rewritten paragraph:

Also, at a time of playing a content once stored, decryption unit 217 reads *ID_2* from ID storage unit 211, reads CSI from CSI storage unit 208, and concatenates the ~~reads~~ read *ID_2* and CSI in the stated order to generate a decryption key *b*. Decryption unit 217 performs decryption algorithm *D* on encrypted content key *b* read from content-key storage unit 219, using the generated decryption key *b*, to obtain a content key, and outputs the obtained content key to decryption unit 220.

Please replace the paragraph beginning at line 3 on page 30 with the following rewritten paragraph:

On receipt by input unit 213 of an input indicating to acquire and accumulate contents, control unit 201 conducts the same processing as above to acquire contents. Once contents have been acquired, control unit 201 has decryption unit 217 decrypt encrypted content key *s* received from AD server 100, ~~and~~ controls encryption unit 218 to encrypt the decrypted content key, and stores the encrypted content key in content-key storage unit 219 as encrypted content key *b*. Also, on receipt of encrypted contents from AD server 100, control unit 201 stores the encrypted contents in content storage unit 209.

Please replace the paragraph beginning at line 3 on page 32 with the following rewritten paragraph:

On-vehicle device 300 is a computer system ~~the same~~similar to AD server 100, and a computer program is stored on the RAM or the hard disk unit of the on-vehicle

device 300. On-vehicle device 300 carries out functions as a result of the microprocessor operating in accordance with the computer program.

Please replace the paragraph beginning at line 6 on page 41 with the following rewritten paragraph:

Device B, having ~~receiving~~ received PKC *Cert_A*, conducts signature verification by performing a signature verification algorithm *V* on signature data *Sig_CA* included in the PKC *Cert_A*, using a public key *PK_CA* of the CA (step S13). If verification is unsuccessful (step S14 = NO), device B ends the processing. If verification is successful (step S14 = YES), device B reads a CRL (step S15), and judges whether *ID_A* included in the received PKC *Cert_A* is registered in the CRL (step S16). If judged to be registered (step S16 = YES), device B ends the processing. If judged to be not registered (step S16 = NO), device B reads PKC *Cert_B* of device B (step S17), and transmits the read PKC *Cert_B* to device A (step S18).

Please replace the paragraph beginning at line 1 on page 43 with the following rewritten paragraph:

Device B, on receipt of random number *Cha_A* concatenates the received *Cha_A* and CSI in the stated order to generate *Cha_A* || *CSI* (step S32), performs signature algorithm *S* on the generated *Cha_A* || *CSI* using a secret key *SK_B* of device B to generate signature data *Sig_B* (step S33), and transmits the generated signature data *Sig_B* to device A (step S34).

Please replace the paragraph beginning at line 23 on page 59 with the following rewritten paragraph:

In this case, on-vehicle device 300, which has IC card 400 connected thereto, is operated to transmit a withdrawal request to IC card 400, and IC card 400 establishes a SAC to confirm that on-vehicle device 300 is registered, and transmits a deletion notification to on-vehicle device 300. On-vehicle device 300 deletes the

CSI, and transmits a deletion-completed notification to IC card 400. IC card 400, on receipt of the deletion-completed notification, stores the ID of the withdrawn on-vehicle device 300. IC card 400, when connected to AD server 100, notifies AD server 100 that on-vehicle device 300 has withdrawn and ~~of~~ the ID of on-vehicle device 300. AD server 100 deletes the ID of on-vehicle device 300 from DEVICE ID in the registration information, subtracts "1" from the registered number, and adds "1" to the remaining number.

Please replace the paragraph beginning at line 21 on page 65 with the following rewritten paragraph:

Also, although in the above embodiment, authentication is conducted in both directions (i.e. mutually), authentication may be only unidirectional.

Please replace the paragraph beginning at line 1 on page 70 with the following rewritten paragraph:

Moreover, client devices may be provided in advance with a priority level, and priority can be given to the registration of devices having a high priority level. Also, when the combined number of client devices newly registered in AD servers T and U exceeds the maximum number, priority may be given to the registration of devices having a high priority level, or a user may ~~selected~~ select devices to be registered.

Please replace the paragraph beginning at line 11 on page 72 with the following rewritten paragraph:

In this way, it is possible to specify which authorized domain the content issued from, in the event of a content decrypted by a client device being improperly distributed outside of the authorized domain within which it originated. Furthermore, when a server that delivered the content manages the ID of client devices registered in various authorized domains, the ID of the client device that issued the content may be included in the CRL.

Please replace the paragraph beginning at line 6 on page 73 with the following rewritten paragraph:

A device on the receiving end, on acquiring the encrypted content and encrypted content key, generates, based on the CSI, a decryption key the same as the encryption key, decrypts the encrypted content key using the decryption key to obtain a content key, and decrypts the encrypted content using the content key to obtain a content.

Please replace the paragraph beginning at line 21 on page 74 with the following rewritten paragraph:

(26) Although in the above embodiment, AD server 100 permits IC card 400 to copy CSI one time, AD server 100 may permit a plurality of copies.

Please replace the paragraph beginning at line 18 on page 75 with the following rewritten paragraph:

On-vehicle devices 602, 603 and 604, which are not registered in AD server 600, are mounted in a vehicle owned by the user. On-vehicle devices 603 and 604 do not

function to communicate directly with AD server 600. On-vehicle device 602 is portable and does function to communicate directly with AD server 600. Also, on-vehicle devices 602, 603 and 604 are connected to and can communicate with each ~~another~~ other.

Please replace the paragraph beginning at line 22 on page 77 with the following rewritten paragraph:

On-vehicle device 602, before registering, acquires the IDs of on-vehicle devices 603 and 604. On-vehicle device 602, at a time of registering, transmits the acquired IDs and the ID of on-vehicle device 602 to AD server 600. AD server 600 stores the received IDs as device IDs. Also, if the remaining number is less than the desired number, AD server 600 stores, from the received IDs, IDs for how ever many devices ~~is~~ are shown by the remaining number. In this case, the user may select which IDs to register, or each ID may have a priority level, and IDs stored in a descending order of priority.

Please replace the paragraph beginning at line 4 on page 88 with the following rewritten paragraph:

Also, the present invention is a member device that uses a content after registering in a group managed by a group management device, and includes a requesting unit operable to request the group management device for registration to the group; a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, common secret information unique to the group; and a holding unit operable to hold the received common secret information.

Please replace the paragraph beginning at line 14 on page 90 with the following rewritten paragraph:

Also, in the member device, the requesting unit may request the group management device for withdrawal from the group, the receiving unit may receive from the group management device, a notification indicating to delete the common secret information, and the holding unit may delete the held common secret information and reactivate the first initial value.

Please replace the paragraph beginning at line 12 on page 93 with the following rewritten paragraph:

Here, in the group management device, the communication unit may output to another group management device, a request inquiring whether the member device is registerable in the other group management device, the other group management device may receive the inquiry request, judge whether a registered number of member devices is less than a maximum number of member devices registerable with the other group management device, and when judged in the affirmative, register the member device and output the common secret information to the group management device, and the communication unit, on receipt of the common secret information from the other group management device, may output the received common secret information to the member device.

Please replace the paragraph beginning at line 23 on page 95 with the following rewritten paragraph:

Here, in the group management device, the reception unit, after the outputting of the common secret information, may receive from the member device, a request for withdrawal from the group, the communication unit, on receipt by the reception unit of the withdrawal request, may output to the member device, a notification indicating to delete the common secret information, the reception unit may receive from the member device, a notification showing that deletion of the common secret information has been completed, and the judging unit, on receipt by the reception unit of the deletion-completed notification, may reduce the registered number.

Please replace the paragraph beginning at line 11 on page 96 with the following rewritten paragraph:

Also, in the member device, the requesting unit may request the group management device for withdrawal from the group, the receiving unit may receive from the group management device, a notification indicating to delete the common secret information, and the holding unit, on acquisition of the deletion notification by the receiving unit, may delete the held common secret information.

Please replace the paragraph beginning at line 17 on page 104 with the following rewritten paragraph:

Also, in the member device, the holding unit may hold an identifier unique to the member device, the communication unit may acquire, from the other member device, an identifier unique to the other member device, and the requesting unit may transmit the held and acquired identifiers to the group management device.

Please replace the paragraph beginning at line 22 on page 106 with the following rewritten paragraph:

Here, in the group management device, when the group management device is determined to be a new group management device for managing a new group formed by combining groups managed by a plurality of group management devices, the communication unit may output to member devices registered in the groups, new common secret information unique to the new group, and when one of the other group management devices is determined to be the new group management device, the group management device may further include a receiving unit operable to receive the new common secret information from the other group management device; and a holding unit operable to hold the received new common secret information.

Please replace the paragraph beginning at line 19 on page 109 with the following rewritten paragraph:

Also, the member device may further include a dividing unit operable, after the holding of the common secret information, and when the member device is determined by the group management device to be another group management device, to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device; and a communication unit operable to output to the member devices to be registered in the other group, common secret information unique to the other group.

Please replace the paragraph beginning at line 6 on page 110 with the following rewritten paragraph:

Also, the member devices registered in the group may each have a priority level, and in the member device, the receiving unit may acquire the priority levels of the other member devices, and the dividing unit may conduct the dividing based on the acquired priority levels.

Please replace the paragraph beginning at line 14 on page 113 with the following rewritten paragraph:

Also, the present invention is a registration device for registering a member device in a group managed by a group management device, the registration device including: a holding unit operable to receive, from the group management device, and hold, common secret information unique to the group; and a notifying unit operable, when the registration device is connected to the member device, to notify the common secret information to the member device.

Please replace the paragraph beginning at line 11 on page 114 with the following rewritten paragraph:

Here, the registration device may further include a reception unit operable to receive, from the member device, a request for acquisition of the common secret

information, and the notifying unit may notify the common secret information to the member device when the acquisition request is received by the reception unit.